MULTIMEDIA UNIVERSITY

FINAL EXAMINATION

TRIMESTER 1, 2018/2019

## TNS3131 – NETWORK SECURITY AND MANAGEMENT
(All sections / Groups)

13 October 2018
9.00 a.m. – 11 a.m.
(2 hours)

INSTRUCTIONS TO STUDENTS

1. This Question paper consists of 5 pages **including cover page with 5 questions.**

2. Attempt **ALL questions.** All questions carry equal marks and the distribution of the marks for each question is given.

3. Please print all your answers in the Answer Booklet provided.

QUESTION 1

a) Define *active attack*. List **FOUR (4)** examples of active attacks.   [3 marks]

b) Briefly explain **SIX (6)** security services.   [3 marks]

c) Given the following model for network security, identify **FOUR (4)** basic tasks in designing a particular security service.
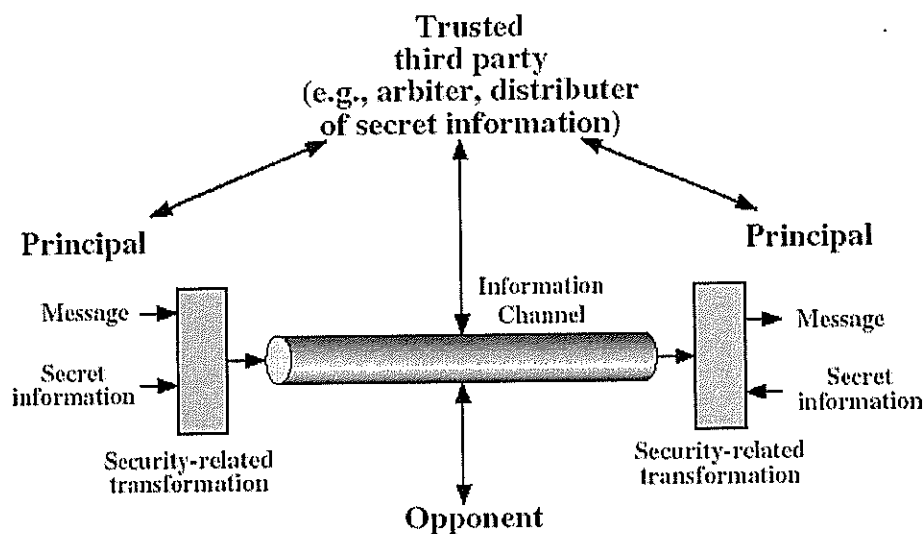
[2 marks]

d) Given the following table, name the types of cryptanalytic attacks based on the amount of information known to the cryptanalyst.   [2 marks]

	Known to Cryptanalyst	Type of Attack
1	• Encryption algorithm • Ciphertext	
2	• Encryption algorithm • Ciphertext • One or more plaintext-ciphertext pairs formed with the secret key	
3	• Encryption algorithm • Ciphertext • Ciphertext chosen by cryptanalyst, together with its corresponding decrypted plaintext generated with the secret key	
4	• Encryption algorithm • Ciphertext • Plaintext message chosen by cryptanalyst, together with its corresponding ciphertext generated with the secret key	

Continued ....

QUESTION 2

a) Feistel proposed the use of a cipher that alternates substitutions and permutations.
   i)   Define *substitution* and *permutation*.   [2 marks]
   ii)   Given the following table, briefly explain the design elements of Feistel cipher.   [2 marks]

	Design Element	Explanation
1	Block size	
2	Key size	
3	Number of rounds	
4	Subkey generation algorithm	

b) A typical stream cipher encrypts plaintext one bit or one byte at a time.
   i) Describe **THREE (3)** design considerations for a stream cipher.   [3 marks]
   ii) Provide a potential advantage of a stream cipher as compared to block cipher.
                                                                                 [1 mark]

c) List the functions of public key and private key involved in public-key cryptography.   [2 marks]

QUESTION 3

a) Discuss the environmental differences between Kerberos version 4 and 5 in terms of encryption system dependence, ticket lifetime, and authentication forwarding.
                                                                                [3 marks]

b) Illustrate the format of X.509 certificate.   [2 marks]

c) Describe **FOUR (4)** processes for Authentication, Authorization and Accounting (AAA).   [2 marks]

d) Given binary input data 00100111 01001100 00010000, identify the character representation for Radix-64 encoding (Refer appendix for Radix-64 table).
                                                                                [3 marks]

QUESTION 4

a) Briefly explain **FOUR (4)** reasons Pretty Good Privacy (PGP) has grown explosively and widely used.
[2 marks]

b) Define *S/MIME*. Explain the difficulties in deploying S/MIME in practices.
[3 marks]

c) Compare *Transport Mode* and *Tunnel Mode* in terms of delivery services and IP packet protection.
[2 marks]

d) i) Define Secure Electronic Transactions (SET). [1 mark]
   ii) Illustrate how SET works. [2 marks]

QUESTION 5

a) Provide **THREE (3)** comparisons for Simple Network Management Protocol (SNMP) version 1 and version 2.
[3 marks]

b) List **THREE (3)** intrusion techniques for password guessing. [1.5 marks]

c) Describe **THREE (3)** importance of intrusion detection. [1.5 marks]

d) Explain **FOUR (4)** phases of typical virus or worm operations. [2 marks]

e) In the table format given below, list one advantage and one disadvantage for the listed firewall methods.
[2 marks]

Types of Firewalls	Advantages	Disadvantages
Packet-filtering routers	•	•
Application-level gateways	•	•

Appendix:

Radix-64 table

6-Bit Value	Character Encoding	6-Bit Value	Character Encoding	6-Bit Value	Character Encoding	6-Bit Value	Character Encoding
0	A	16	Q	32	g	48	w
1	B	17	R	33	h	49	x
2	C	18	S	34	i	50	y
3	D	19	T	35	j	51	z
4	E	20	U	36	k	52	0
5	F	21	V	37	l	53	1
6	G	22	W	38	m	54	2
7	H	23	X	39	n	55	3
8	I	24	Y	40	o	56	4
9	J	25	Z	41	p	57	5
10	K	26	a	42	q	58	6
11	L	27	b	43	r	59	7
12	M	28	c	44	s	60	8
13	N	29	d	45	t	61	9
14	O	30	e	46	u	62	+
15	P	31	f	47	v	63	/
						(pad)	=

End of Paper.